White Paper

Intel® Transparent Supply Chain

Ensuring Device Security from the Factory Floor Through End of Life

Building a Trusted Supply Chain based on a hardware Root of Trust is key to helping prevent product tampering and unauthorized substitutions.

Author

Tom Dodson

Supply Chain Security Architect

Executive Summary

With the expansion of data centers, cloud computing, and the Internet of Things, ensuring trust in the supply chain has become more important than ever. A supply chain based on the Intel® Transparent Supply Chan Service can enhance security for everything from sourcing components to distribution of the final product.

This paper describes the incentives for organizations to prioritize supply chain trust and introduces the Intel® Transparent Supply Chain (Intel® TSC) service. It also explains the use of a hardware root of trust to establish a trusted supply chain.

Supply Chain Security is a Concern Across Public and Private Sectors

Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain.

— National Institute of Standards and Technology

Incentives for Supply Chain Trust

The use of technology to compromise supply chains is not a new phenomenon; one article in Supply Chain 24/7 provides a history of supply chain cyberattacks dating back to the Cold War.[1] Before end users even turn on their new equipment, malicious actors have numerous opportunities to disrupt and compromise the supply chain tasked with delivering new devices into end users' hands. Such attacks should concern every company regardless of their size or market focus.

The U.S. government is well aware of the significance of the problem: A paper from the National Institute of Standards and Technology2 (NIST) states that "Federal agencies are concerned about the risks associated with information and communications technology products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain."[2]

In 2015, the U.S. Department of Defense published a three-page interim rule to the Defense Federal Acquisition Regulation Supplement. This interim rule gave government contractors a deadline to implement the requirements of the Special Publication 800-171,[3] which NIST published to counteract cybersecurity threats. Section 252.246-7007 of this document, Contractor Counterfeit Electronic Part Detection and Avoidance System, specifically addresses "design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts."[4]

Today, instances of attacks on supply chains and the use of counterfeit, substituted, or malicious components abound. In a May 2020 brief, Deloitte reported that

Table of Contents

Executive Summary 1

Supply Chain Security is a Concern Across Public & Private Sectors 1

Incentives for Supply Chain Trust..... 1

Intel® Transparent Supply Chain..... 2

TPM as the Hardware Root of Trust... 2

Implementing Trusted Supply Chain. 3

Platform Certificate and Appliance Certificate 3

"As-built Data": System Ingredients .. 5

Conclusion 6

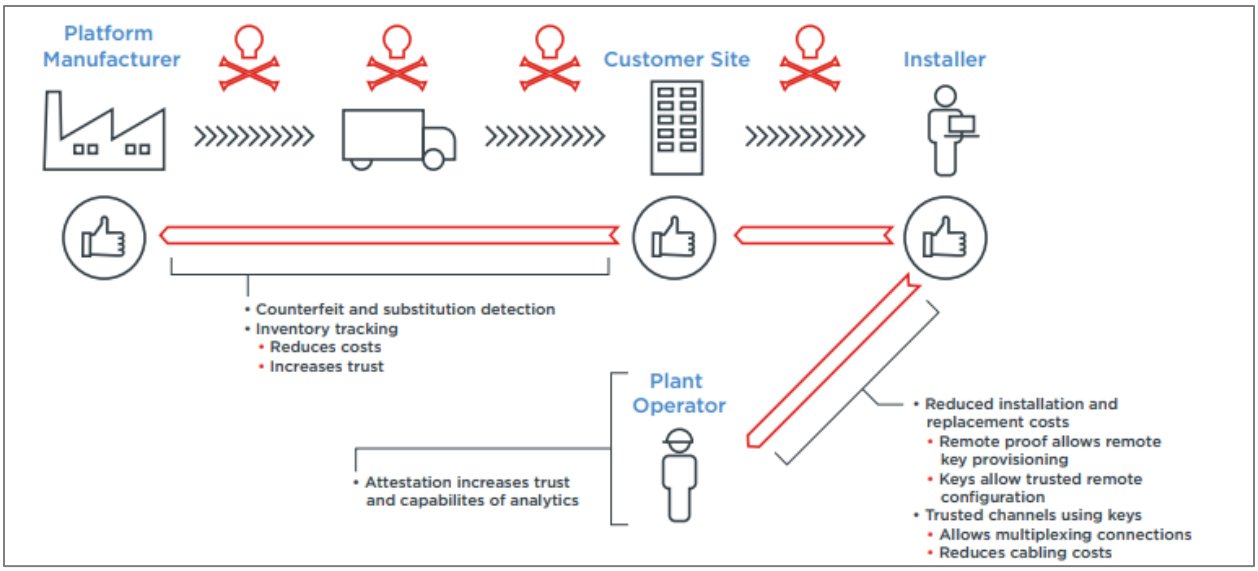


Figure 1. The Intel® Transparent Supply Chain value proposition

"4 in 10 manufacturers surveyed indicated that their operations were affected by a cyber incident in the past 12 months."[5] According to the brief, the manufacturing industry is one of those most frequently targeted in cyberattacks, with attacks on supply chains having increased just between March and May of this year.

The diversity of today's manufacturing, logistics, and inventory environments makes information about a device's origin and subsequent history especially critical for organizations and end users.

In particular, remote deployment and provisioning present both challenges and opportunities for supply chain security: They introduce new vulnerabilities to cyberattacks but can also decrease service costs and reduce the steps needed to physically track devices. As such, organizations stand to benefit from a trusted supply chain that enables remote deployment and provisioning of end-user devices.

Intel® Transparent Supply Chain

Intel® TSC is a service enabling visibility and traceability of hardware components, firmware, and systems on compute devices. TSC offers customers the following benefits:

Component-level Traceability

- Enterprise procurement can ensure that the system they received is the one that was ordered without any counterfeit parts
- Signed Platform certificate that conforms to Trusted Computing Group (TCG) Platform Certificate v1.1 Specification[6] providing provenance and confidence in the authenticity of their systems

Tamper Detection

- At provisioning, the benefit of matching current state against configuration at manufacturing to help identify tampering
- Capability to compare state after international travel with known good state to detect changes
- Benefit of ensuring returned product is the same quality as the original sent to customer

Fleet-level Insights

- Ability to correlate data from internal ticketing database against supplier platform information
- Benefit of knowing systems impacted by published vulnerabilities and quickly updating the subset of affected systems

Intel® TSC leverages three innovations to deliver this platform traceability and transparency:

- The TCG Trusted Platform Module
- The TCG Platform Certificate
- "As-built" data
- The Statement of Conformance
- TSC AutoVerify Tools

Intel® TSC: TPM as the Hardware Root of Trust

Assurances of a device's origin help establish the foundation for a trusted supply chain. The Trusted Computing Group's initial Trusted Platform Module (TPM) standard defined a hardware root of trust. More recently, Trusted Platform Module 2.0, now the International Organization for Standardization (ISO) standard (ISO 11889)[7] created a library specification to describe all the commands and/or features that could be implemented or needed in a variety of platforms, including embedded systems.

In the Trusted Platform Module, the Endorsement Key (EK) is a permanent key (with some exceptions) that is uniquely associated with a specific Trusted Platform Module. It provides assertions about the Trusted Platform Module but no assertions about the platform. A Trusted Platform Module EK can certify other TPM and/or platform keys created by the

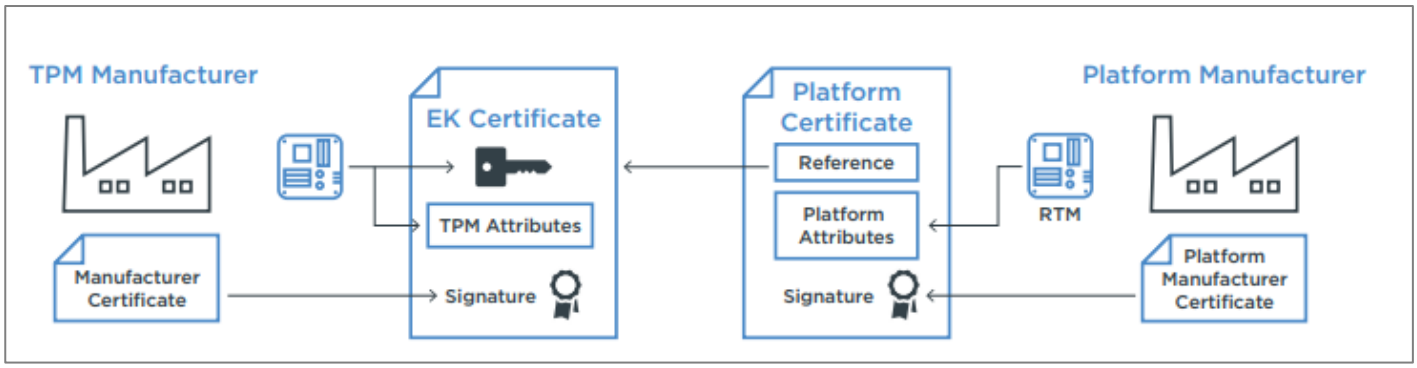


Figure 2. The TPM general architecture transfers keys and certificates to build trust

owner or users. In addition, it also has Platform Configuration Registers, Attestation ID Keys, Signature Keys, and Encryption Keys for verifying access and protecting data.

Figure 2 shows how Intel® TSC utilizes the TPM to provide the hardware root of trust. Its EK certificate and a platform certificate are used to establish the documentation for the platform.

The Trusted Platform Module's EK certificate is signed by the TPM vendor. Next, the Platform Manufacturer attaches the TPM to a platform where the EK is bound to the platform to provide a platform specific key. The platform certificate created by the platform manufacturer attributes asset information about the platform and the Root of Trust for Measurement (RTM), binding it to the TPM.

The value of the measurements is proportional to the trust in the RTM provided by the platform manufacturer. Finally, the supply chain obtains proof of assertions to verify platform and Encryption Key certificate signatures, as well as to verify the TPM EK certificate bound to that platform.

Implementing a Trusted Supply Chain

Building on the TPM general architecture, Figure 3 shows the steps for the documentation for the root of trust, which continues through the supply chain until it gets to the final owner, where an IT expert uses open-source tools to verify platform signatures and TPM EK certificates, as well as conduct other trust-confirming tasks.

Intel® TSC: Platform Certificate and Appliance Certificate

Intel® TSC also delivers TCG Platform Certificates and Appliance Certificates as critical assets to deliver supply chain transparency, traceability, and enhanced trust. The TCG Platform Certificate helps to ensures a computing device is trustworthy and secure. It is used to verify that a device's hardware and software components have not been tampered with or compromised. The form and function of the Platform Certificate is described in the TCG Platform Certificate Profile Specification v1.1.

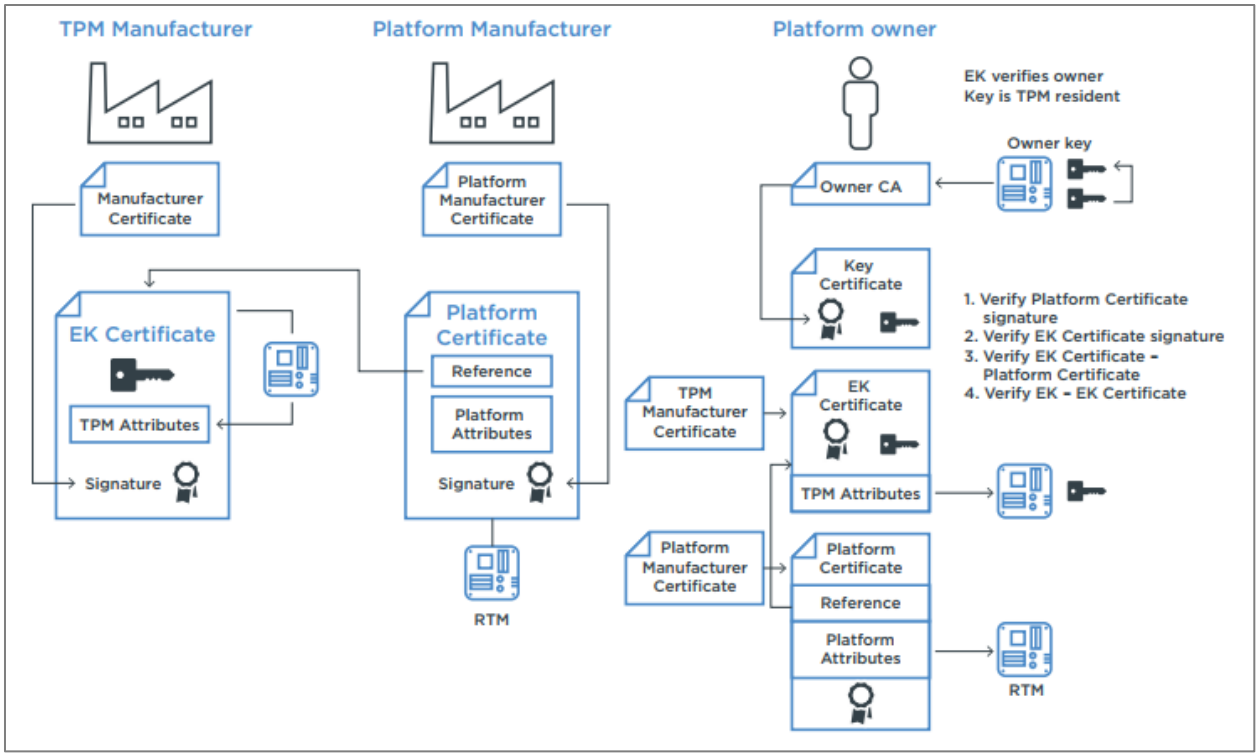


Figure 3. Intel® TSC traceability extends to the platform owners and users

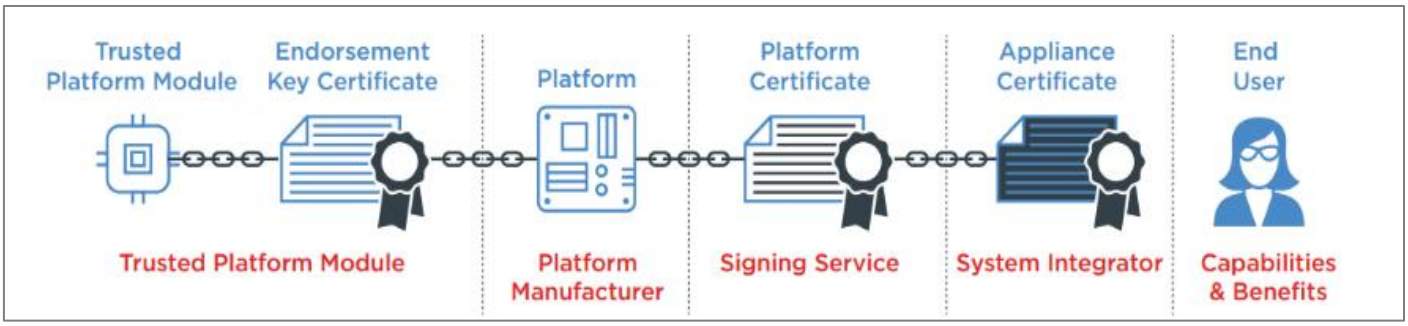


Figure 4. Generating the chain of trust in a typical system touches each stage

The certificate is issued by a trusted authority and is made available for the device by Intel, providing a way for other systems and applications to trust the device. In the case of Intel® TSC, the trusted authority is Digital Content Protection, LLC (DCP), a wholly owned subsidiary of Intel. DCP is an organization that licenses technologies and preforms key generation for a variety of applications such as for protecting premium commercial entertainment content.

Based on the previous chain established in the lifecycle of the system, Figure 4 shows how Platform Certificates are generated. Generating the chain of trust starts with the TPM, creating the EK for each TPM and establishing the hardware root of trust. Next, the platform manufacturer permanently mounts the TPM onto the platform, creates the platform certificate, and binds it to the EK.

DCP provides a platform certificate that cryptographically binds the platform to the EK. Finally, the System Integrator creates an Appliance Certificate and binds it to the Platform Certificate. At the end of the process, the end user benefits from the ability to trace the appliance to credible hardware root of trust, establishing technology provider accountability as well as transparency.

The chain of trust process in Intel® TSC is important and essential to provide total traceability and a HRoT based on the TPM. It enables component-level traceability for platforms and systems to mitigate the risk of counterfeit electronic parts while conforming to DFARS Supplement 246.870-2.

Intel® TSC also provides an end-user the TSC AutoVerify tool that identifies certain system changes from the time of manufacturing to the time of first boot. The "As-Built" data report and TSC AutoVerify tool offers customers confidence in the authenticity of their systems.

Traceability in the supply chain includes platform certificates with component level traceability supported by an "as-built" report generated from the factories, a statement of conformance attesting to the authenticity of the system and finally the customer web portal that downloads the files with a link sent regarding access details to the files/certificates.

Figure 5 shows how the various trust items flow through the Intel® TSC process from initial generation, signed and then downloaded so the customer can use the tool to verify it.

System-level traceability is based and begins with the HRoT provided by the TPM on the motherboard. In addition, Intel software tools are deployed during manufacturing to capture system information and the Trusted Platform Module certificate (including the public EK). A unique X.509 Platform Certificate for each system is generated and signed using DCP as the Platform Manufacturer Certificate Authority. This attests that the purchased system is the specific system built by the manufacturer. To aid in the process, Intel makes available the TSC AutoVerify tools so that IT, datacenter, and CSP customers can utilize the supply chain assets delivered via Intel® TSC. Figure 6 shows how data from original and as-delivered platform snapshots are identified and displayed.

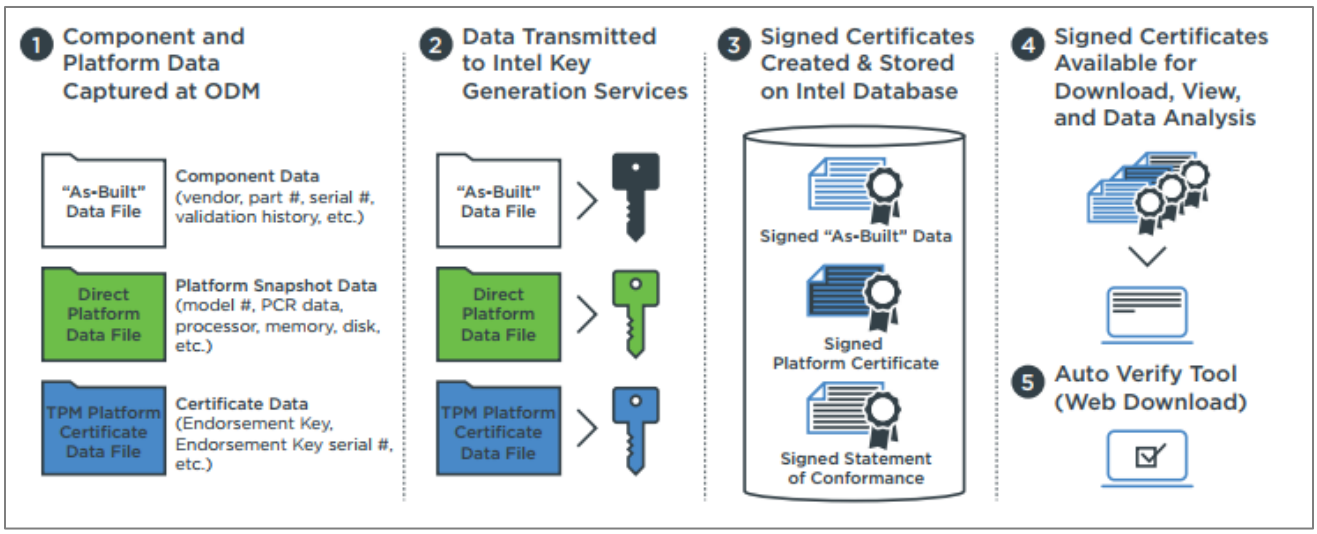


Figure 5. Intel® TSC uses the HRoT in the TPM, Platform Certificates, and other data confirmed by the AutoVerify tool

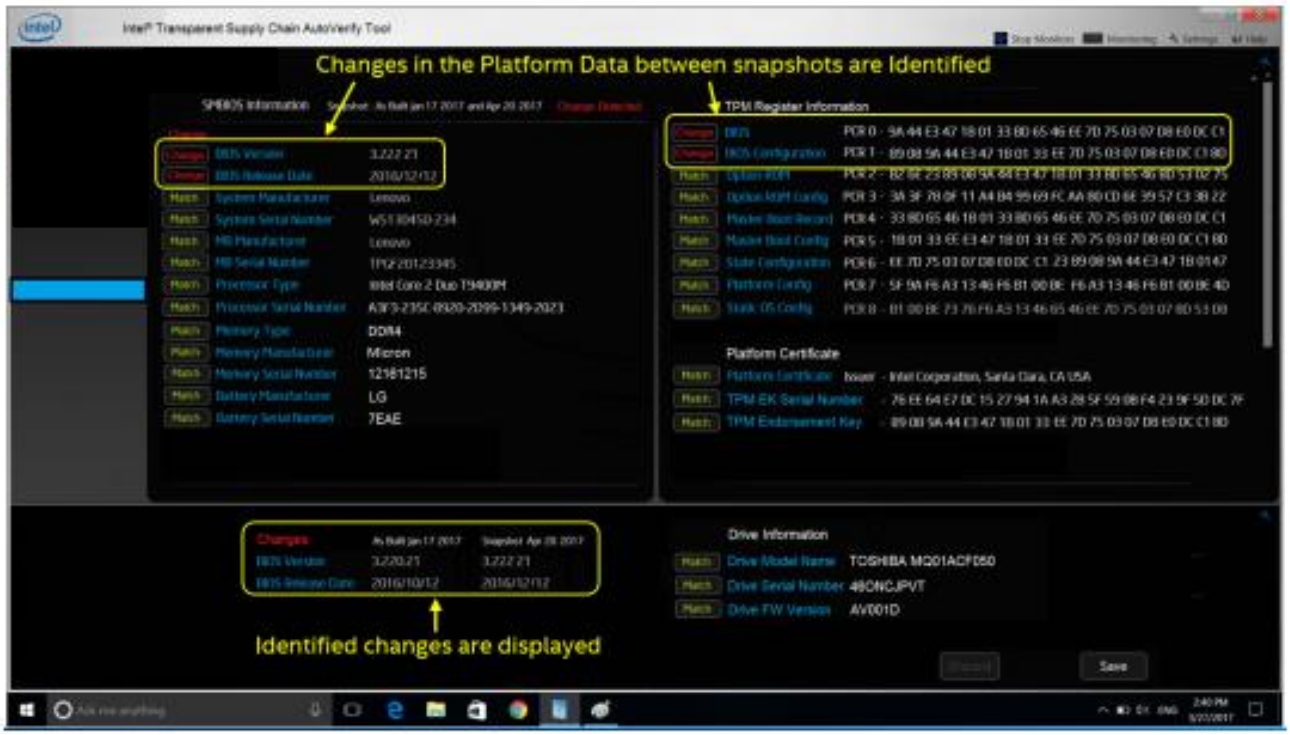


Figure 6. The TSC AutoVerify tool communicates identified changes and other crucial data to end-user certificates

Intel® TSC "As-built Data": System Ingredients

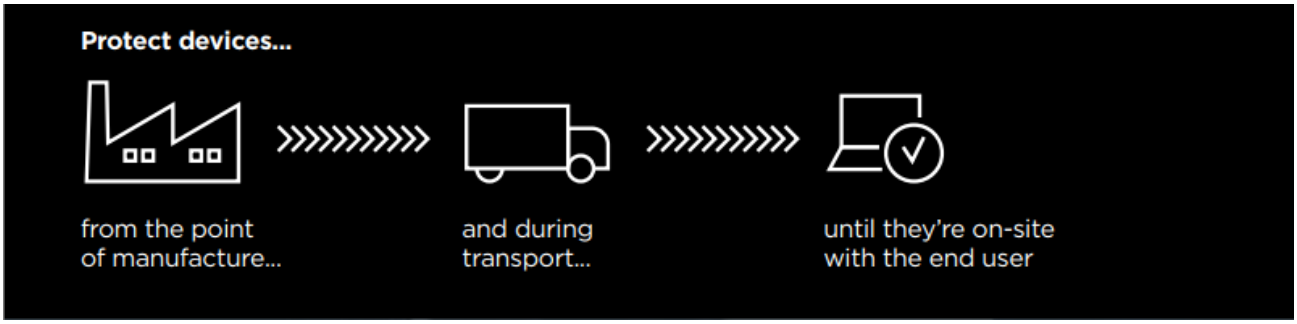
Transparency must include a summary of the active components used to create the system. Some active components such as the CPU, memory, and drives communicate electronically with the SMBios and are captured within the Platform Certificate. Passive component and active components that do not that do not communicate to the SMBios are captured within the "As-built" report (or ABD) in the Intel® TSC Service.

The ABD contains the sourcing details for the components that have been used to build the product. These components include bare PCB, capacitors and resistors, and active components such as transistors, FETs and ICs. The report also includes the image source file name and the checksums of the programable devices. The ABD is collected from the OEM and ODM shop-floor control system and contains up to 24 data fields for each component including: Serial number, product ID, manufacturer, lot code, and whether the component was purchased directly or through a distributor – and the name of the distributor in the event of the later. Procuring parts from an authorized distributor of that manufacturer is a new requirement of DFARs section 246.870-2

Intel® TSC brings security into the supply chain transport and delivery cycle with a documented, auditable program that enables traceability of all purchases at the component and system level.

A trusted supplier guarantee ensures that all suppliers adhere to Intel's strict manufacturing standards and pass quarterly compliance and security assessments, while a TSC AutoVerify tool identifies certain system changes from the time of manufacturing to the time of first boot. The Customer Web Portal allows convenient access to signed files verifying integrity, such as:

- A signed Platform Certificate that links to a TPM on the device's motherboard
- "As-built" data reports that provide users with information on key system components (such as the manufacturer, part number, batch number, and distributor)
- A statement of conformance, signed by Intel, which guarantees the authenticity of the systems
- Intel® TSC AutoVerify Tools to compare the 'as-manufactured' data sets with a current platform snapshot of the system



Conclusion

Product tampering and unauthorized substitutions can occur anywhere in the supply chain. Intel has introduced Intel® Transparent Supply Chain with our supporting OEM and ODM partners as a service to enhance end-to-end device security. With trusted supply chain assurances in place, companies can reduce the risk of supply chain tampering and minimize the chance of receiving counterfeit parts—ultimately protecting valuable company data. This paper explored the mechanics underpinning of the Intel® TSC service: namely, a trusted supply chain (based on a hardware Root of Trust established by using the Trusted Computing Group's Trusted Platform Module standard) and an Auto-Verify tool (which provides traceability, accountability, assurance, and security to the user) to establish trust in the supply chain and mitigate the potential for cyberattacks due to supply chain tampering.

Steps to Establish Supply Chain Trust

Immediately evaluate your company's supply chain for its IT components

Within three months identify IT components that have supply chain risk and determine if there is an opportunity to incorporate TSC supply chain

Within six months implement a secure supply chain based upon the TPM

Future purchases consider platforms that incorporate Lenovo models with the Intel® Transparent Supply Chain Certification Tools for TPM 2.0 Support

About the Author

Tom Dodson has been in the Supply Chain Security field for the past 24 years working with component suppliers and system manufacturers to ensure a secure and healthy supply chain has been established. Over the last five years, Tom has helped develop Intel® Transparent Supply Chain and has worked with NIST and TSC to establish standards that can be used across the industry.

[1] http://www.supplychain247.com/article/the_supply_chain_silent_threat_cyber_attack/security
[2] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf
[3] https://www.eventtracker.com/campaigns/nist-800-171-compliance
[4] https://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm#252.246-7007
[5] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/Deloitte-Global-Cyber-COVID-19-Executive-Briefing-Issue-5-release-date-5.6.2020.pdf
[6] https://trustedcomputinggroup.org/resource/tcg-platform-certificate-profile/
[7] https://www.iso.org/standard/66510.html